Title: Homomorphic encryption schemes

Author: Anežka Titěrová

Department: Department of Algebra

Supervisor: RNDr. Alexandr Kazda, Department of Algebra

Abstract: Rivest et al. posed in 1978 the cryptographic problem how to correctly compute arbitrary functions over encrypted data without direct decrypting. This problem is solved by using of a fully homomorphic encryption scheme, which was discovered and first described by Craig Gentry in 2009.

This work gives a summary of contemporary knowledge in this field. The attention will be restricted to a general overview how to construct the fully homomorphic encryption scheme with respect to the information security. The results will be applied in an implementation of a somewhat homomorphic encryption scheme as a computer program.

Fully homomorphic encryption schemes have abundant applications, especially in secure cloud computing. Nevertheless, the greatest challenge for scientists is finding out more efficient algorithm because existing implementations are not as effective and fast as required for everyday use.

Keywords: homomorphic encryption, fully homomorphic encryption scheme, lattice cryptography, logic circuit